UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/666,140	09/20/2000	Joseph G. Barrett	24838-0003001	5787

26171 7590 11/09/2009

FISH & RICHARDSON P.C.
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
NGUYEN, VAN KIM T	
ART UNIT	PAPER NUMBER
2456	

NOTIFICATION DATE	DELIVERY MODE
11/09/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PATDOCTC@fr.com

Office Action Summary	Application No.	Applicant(s)	
	09/666,140	BARRETT ET AL.	
	Examiner	Art Unit	
	Van Kim T. Nguyen	2456	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 June 2009*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1,3,4,6-14,25-41 and 45-58* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1,3,4,6-14,25-41 and 45-58* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *July 9, 2009*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. This Office Action is responsive to communications filed on June 5, 2009.

Claims 15-24 and 42-44 have been cancelled, new claims 46-58 added, thus claims 1, 3-4, 6-14, 25-41 and 45-58 remain pending in the case.

Information Disclosure Statement

2. The information disclosure statement (IDS) submitted on July 9, 2009 is in compliance with the provisions of 37 CFR 1.97. Accordingly, the information disclosure statement is being considered by the examiner.

Response to Arguments

3. Applicant's arguments with respect to claims 1, 3-4, and 6-14, 25-41 and 45-58 have been considered but are moot in view of the new grounds of rejection.

Claim Rejections - 35 USC § 103

4. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

5. Claims 1, 3-4, and 6-14, 25-39 and 45-58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Belissent (U.S. Patent No. 6,789,203), in view of Porras et al. (US 6,484,203), hereinafter Stone.

Regarding claim 50, Belissent teaches a switch comprising:

a processor (212, 700, Figures 2 and 7; col. 5: lines 52-56, and col. 7: lines 18-60); and

a memory (214, 704, 706, 708; Figures 2 and 7; col. 5: lines 56-61 and col. 7: lines 20-39) encoded with machine readable instructions that, when executed by the processor, operate to cause the processor to perform operations comprising:

transferring data to and from access provider (col. 7: lines 46-53);

monitoring, at the switch, for connection transaction between multiple an access requestor and the access provider (col. 5: lines 45-61);

based on the monitoring, determining, by the switch, whether a cumulative number of connection transactions initiated to the access provider by an attacking access requestor during a first period of time exceeds a threshold number (col. 5: line 52—col. 6: line 17); and

denying, at the switch, access by the attacking access requestor to the access providers in response to a determination that the cumulative number of connection transactions initiated to the access provider by the attacking access requestor exceeds the threshold number during the first period of time (col. 5: line 65 – col. 6: line 10).

Belissent does not explicitly call for determining the connection transactions initiated to more than one access providers.

Porras teaches determining the connection transactions initiated to more than one access providers (enterprise monitor 16f can be used to monitor across domains for global correlation; col. 3: line 40 - col. 4: line 4).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to apply Porras' global monitoring technique in Belissent's system in order to improve system security.

Claims 1 and 25 are rejected under the same basis.

Regarding claim 3, Belissent-Porras also discloses the monitoring further includes counting, using the switch, and comparing the number of connection transactions initiated by the access requestor to any of the access providers through the switching component during the first configurable period of time to the configurable threshold (Belissent; col. 5: line 52 – col. 6: line 10).

Regarding claim 4, Belissent-Porras also discloses:

comparing, using the switch, the number of connection transactions initiated by the access requestors through the switch during the first period of time to the threshold number (Belissent; col. 5: line 52 – col. 6: line 10).

Claim 26 is rejected under the same basis.

Regarding claim 6, Belissent-Porras also discloses counting, using the switch, the cumulative number of connection transactions initiated to any of the access providers by the attacking access requestor during the first period of time such that the cumulative number of connection transactions reflects connection transactions initiated to all of the access providers by the attacking access requestor (since a monitor 16 can construct interval summary event records and analyze event streams based on different criteria such as source addresses or destination addresses, it is obvious the cumulative number of all connection transactions initiated by an attacking access requestor can be monitored and calculated; Belissent; col. 5: line 52 – col. 6: line 10; and Porras; col. 4: lines 19-60).

Claim 47 and 51 are rejected under the same basis.

Regarding claim 7, Belissent-Porras also discloses:

comparing, using the switch, the cumulative number of connection transactions initiated by the attacking access requestor during the first period of time to the thresho1d number (since a monitor 16 can construct interval summary event records and analyze event streams based on different criteria such as source addresses or destination addresses, it is obvious the cumulative number of all connection transactions initiated by an attacking access requestor can be calculated and compare to the rejection threshold; Belissent; col. 5: line 52 – col. 6: line 10; and Porras; col. 4: lines 19-60); and

denying, using the switch, access by the attacking access requestor to all of the access providers connected to the switch when the comparison results indicate that the cumulative number of connection transactions initiated by the attacking access requestor during the first period of time exceeds the threshold number (Belissent; col. 5: line 52 – col. 6: line 10; and Porras; col. 4: lines 19-60).

Claim 27 and 52 are rejected under the same basis.

Regarding claim 8, Belissent-Porras also discloses the monitoring includes monitoring a computer system for connection transaction made using TCP (Belissent; col. 5: lines 4-45 and Porras; col. 4: lines 19-28).

Claim 28 is rejected under the same basis.

Regarding claims 9 and 29, Belissent-Porras also discloses identifying the IP addresses through the use of a header attached to a message representing the connection transaction being detected (Belissent; col. 5: lines 4-45).

Claim 29 is rejected under the same basis.

Regarding claim 10, Belissent-Porras also discloses denying access to the access providers through the switch by the attacking access requestor for a second configurable period of time after detecting a most recent connection transaction initiated by the attacking requestor through the switch (if during the previous throttling interval, the connection request rate is in excess of the slowdown threshold SLD_t, the IP throttler unit 216 slows down the connection request rate stream by a wait time, Belissent; col. 6: lines 18-40).

Claim 30 and 53 is rejected under the same basis.

Regarding claim 11, Belissent-Porras also discloses resetting the second configurable period of time after detecting a new connection transaction initiated by the attacking access requestor through the switch during the second configurable period of time (when a new connection request has been received, a determination is made as whether or not it is the beginning of a new interval. If it is determined that a new interval has begun, then a new wait time W_t is calculated, Belissent; col. 6: line 57 – col. 7: line 5).

Claims 31-32 and 54 are rejected under the same basis.

Regarding claim 12, Belissent-Porras also discloses denying access to the access providers through the switch by the attacking access requestor for a second configurable period of time after detecting a most recent connection transaction initiated by the attacking access requestor through the switch (if during the previous throttling interval, the connection request rate is in excess of the slowdown threshold SLD_t, the IP throttler unit 216 slows down the connection request rate stream by a wait time, Belissent; col. 6: lines 18-40).

Claim 33 is rejected under the same basis.

Regarding claim 13, Belissent-Porras also discloses the access requestors are clients and the access providers are hosts such that the monitoring includes detecting connections transactions through the switch between multiple clients and multiple hosts (Belissent; col. 5: lines 4-45, and Porras; col. 4: lines 19-60) .

Claim 34 is rejected under the same basis.

Regarding claim 14, Belissent-Porras also discloses counting, using the switch, a cumulative number of connection transactions for all of the access providers connected to the switch initiated by each of the access requestors during the first configurable period of time (since a monitor 16 can construct interval summary event records and analyze event streams based on different criteria such as source addresses or destination addresses, it is obvious the cumulative number of all connection transactions initiated by an attacking access requestor can be monitored and calculated; Belissent; col. 5: line 52 – col. 6: line 10; and Porras; col. 4: lines 19-60).

Claim 35 is rejected under the same basis.

Regarding claims 36, Belissent-Porras also discloses a host computer system receives communication from the switch (Figure 2; Belissent).

Regarding claims 37, Belissent-Porras also discloses the switch is included in a host system (Figure 1; Belissent).

Regarding claim 38, Belissent-Porras also discloses denying, using the switch, access by the attacking access requestor to all of the access providers connected to the switch irrespective of which of the access providers to which the attacking access requestor initiated connection transactions to exceed the threshold (since a monitor 16 can construct interval summary event records and analyze event streams based on different criteria such as source addresses or destination addresses, it is obvious the cumulative number of any or all connection transactions initiated by an attacking access requestor can be monitored and calculated; Belissent; col. 5: line 52 – col. 6: line 10; and Porras; col. 4: lines 19-60).

Regarding claim 39, Belissent-Porras monitoring includes monitoring, using a switch configured to establish communication links between access requestors and access providers, for attempts, by the attacking access requestor, to establish a communication link with any of the access providers (since a monitor 16 can construct interval summary event records and analyze event streams based on different criteria such as source addresses or destination addresses, it is obvious the cumulative number of any or all connection transactions initiated by an attacking

access requestor can be monitored and calculated; Belissent; col. 5: line 52 – col. 6: line 10; and Porras; col. 4: lines 19-60).

Regarding claims 45-46, Belissent-Porras also discloses the access providers include a first access provider (12a) and a second access provider (12b, 12c) that is different from the first access provider (Figure 1), and the monitoring takes into account interactions of the attacking access requestor with both the first access provider and second access provider (since a monitor 16 can construct interval summary event records and analyze event streams based on different criteria such as source addresses or destination addresses, it is obvious the cumulative number of any or all connection transactions initiated by an attacking access requestor to any or all domains can be monitored and calculated; Belissent; col. 5: line 52 – col. 6: line 10; and Porras; col. 4: lines 19-60).

Claim 55 is rejected under the same basis.

Regarding claim 47, Belissent-Porras also discloses determining, by the switch, whether a cumulative number of connection transactions initiated to more than one of the access providers by the attacking access requestor during a first configurable period of time exceeds a configurable threshold number (since a monitor 16 can construct interval summary event records and analyze event streams based on different criteria such as source addresses or destination addresses, it is obvious the cumulative number of any connection transactions initiated by an attacking access requestor, i.e., a source address, to any or all domains, i.e., any destination

addresses, can be monitored and calculated; Belissent; col. 5: line 52 – col. 6: line 10; and Porras; col. 4: lines 19-60).

Claim 56 is rejected under the same basis.

Regarding claim 48, Belissent-Porras also discloses determining, by the switch, whether a total number of connection transactions initiated to all of the access providers by the attacking access requestor during the first period of time exceeds the threshold number (since a monitor 16 can construct interval summary event records and analyze event streams based on different criteria such as source addresses or destination addresses, it is obvious the cumulative number of all connection transactions initiated by an attacking access requestor, i.e., a source address, to any or all domains, i.e., all destination addresses, can be monitored and calculated; Belissent; col. 5: line 52 – col. 6: line 10; and Porras; col. 4: lines 19-60).

Claim 57 is rejected under the same basis.

Regarding claim 49, Belissent-Porras also discloses determining, by the switch, that the cumulative number of connection transactions exceeds the threshold number despite a number of connection transaction initiated to each of the more than one of the access providers individually being less than the threshold number (since a monitor 16 can construct interval summary event records and analyze event streams based on different criteria such as source addresses or destination addresses, it is obvious the cumulative number of all connection transactions initiated by an attacking access requestor, i.e., a source address, to any or all domains, i.e., all destination addresses, can be monitored and compared to the threshold, regardless whether the connection

requests to individual access providers being less than the threshold number; Belissent; col. 5: line 52 – col. 6: line 10; and Porras; col. 4: lines 19-60).

Claim 58 is rejected under the same basis.

6. Claims 40 and 41 are rejected under 35 U.S.C. 103(a) as being unpatentable over Belissent-Porras, as applied to claims 39 and 11, respectively above, and further in view of Lin et al (US 6,751,668).

Regarding claim 40, Belissent-Porras does not explicitly teach the establishment of a communication link between the attacking access requestor and one of the access providers involving exchange of more than two electronic messages.

Lin discloses establishment of a communication link between the attacking access requestor and one of the access providers involving exchange of more than two electronic messages (e.g., SYN and SYN/ACK; Figure 1, col. 2: lines 2-9).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize Lin's method of responding to service attacks in Belissent-Porras' system in order to limiting unwanted access to server data.

Regarding claim 41, Belissent-Porras-Lin also discloses:

determining, using the switch, that the second configurable time period, has passed without detecting a new connection transaction initiated by the attacking access requestor to any of the access providers through the switching component (monitoring the rate of receipt of session establishment; Lin, Figure 2: lines 30-43); and

in response to determining at the second configurable time period has passed without detecting a new connection transaction initiated by the attacking access requestor to any of the access providers through the switching component, allowing access by an attacking access requestor to the access providers (monitoring the rate of receipt of session establishment is less that the MAX_SESS_RATE, the state machine moves back to the normal state 202; Lin, Figure 2: lines 30-43).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize Lin's method of responding to service attacks in Belissent-Porras' system in order to limiting unwanted access to server data.

Conclusion

7. Applicant's amendment necessitated the new grounds of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

8. Any inquiry concerning this communication or earlier communications from the examiner should be directed to VAN KIM T. NGUYEN whose telephone number is (571)272-3073. The examiner can normally be reached on 8:00 AM - 4:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Bunjob Jaroenchonwanit can be reached on 571-272-3913. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Van Kim T. Nguyen
Examiner
Art Unit 2456

vkn

/Bunjob Jaroenchonwanit/

Supervisory Patent Examiner, Art Unit 2456